Gururajan, Raj (2006) *A Discussion on Security Risks in Mobile COMMERCE*. e-Business Review, 7 (2). pp. 9-39. ISSN 1229-6546 . This is the author's final corrected manuscript.

# A DISCUSSION ON SECURITY RISKS IN MOBILE COMMERCE

**RAJ GURURAJAN**
University of Southern Queensland

## ABSTRACT

*Recent technological innovations such as mobile computing have enabled new facility of buying and selling using mobile device. While users welcome this, security risks[i] that can emerge due to this new facility raise concerns. This exploratory research discusses the security risks in mobile computing in terms of direct risks and indirect risk.*

***Keywords**: mobile commerce, security, electronic commerce*

## INTRODUCTION

The advent of mobile computing facilitates the mobility to research, communicate, and purchase goods and services from anywhere at anytime without being tied to a desktop. Using the Internet in conjunction with mobile computing opens up many more activities than merely online purchasing. For instance, mobile applications such as emails, weather reports, sport scores, flight and reservation information, navigational maps, and stock quotes are becoming common. While the dominance of these applications is expected to grow, innovative online applications such as location identification programs will further drive new areas of mobile commerce growth. For instance, the Gartner Group estimated that by the end of this year (i.e. 2004), 40% of consumer-to-business e-commerce will be conducted over Web-enabled phones (Haskin, 1999). Supporting argument for this can also be found in Deitel (2001). It is also expected that by 2008, the number of wireless Internet devices will outnumber wired devices (Deitel & Deitel, 2001).

The advent of e-commerce in conjunction with mobile devices has prompted the idea of mobile commerce, commonly known as m-commerce (Green, 2000). The underlying architecture to support mobile communication is wireless application protocol (WAP). The WAP provides a set of software instructions to communicate in a wireless environment with mobile devices as an interface. To facilitate access to the number of services provided and those envisaged for the future, today's mobile device consists of a full colour graphics display, touch screen, and an in-built Internet browser with an optional limited keypad. The idea is to serve the customer better by providing up-to-date information anywhere, any time, anyhow using the mobile telephone (McConnel, 2000). The basic advantage of m-commerce is its versatility and size (Redman, 2002). Using the mobile devices, the technology facilitates access to information that is on-line and up-to-date.

Mobile communication technology can be categorised into three generations. The first generation of mobile communications was analogue. The second generation used digital encoding. These systems were used mainly for voice. The third generation is designed for high-speed communication, which involves data transfer and voice. This third generation will also support multimedia capabilities. Current m-commerce developments are at this stage (Schiller, 2000).

Despite the technical growth, it appears the telecommunication companies have a stronghold on the development and implementation of the m-commerce (Stuart & Bawany, 2001). The users will be able to access information with the telecommunication networks as a bridge to wired Internet services. Mobile device manufacturers and telecommunication companies have discussed a number of usage models using various protocols such as the "Bluetooth" jointly developed by Nokia, IBM, Ericsson, Intel and Toshiba. These usage models enable end users to choose a device and access of their choice in order to perform mobile commerce oriented activities. In recent months, these usage models also

have driven new applications for users. Examples of these usage models in Australia include Optus Telecommunication network coupled with mobile telephones such as Siemens and Motorola.
The objective of the paper is to provide a comprehensive discussion on security risks in mobile commerce. To achieve this purpose, this paper developed a model taxonomy of security risks based on existing literature. The need for security in m-commerce environment is established initially in this paper. Then, taxonomy of security issues specific to m-commerce is provided. The taxonomy is further discussed in terms of two major sub headings direct threats and indirect threats. These two threats are discussed with a number of sub headings in detail to provide a comprehensive understanding of potential threats in m-commerce environment. The paper is then concluded by providing some brief solutions.

## THE NEED FOR SECURITY IN M-COMMERCE

Currently most mobile devices (laptops, WLANs, personal digital assistants (PDAs), etc) do not contain the same capabilities as mobile phones (e.g. Smart Cards to improve security, roaming to improve remote connectivity), thus limiting their use in wireless environments. The feasibility of combining these technologies for use in a specific setting will be dependent upon the security protocols. It appears that the lack of security provision has created a barrier against the adoption of mobile commerce among users (Hu et al., 2002) and prior research in the area appear to have focussed predominantly on 'wired' environments (Colagiuiri, 1997) with little attention being afforded to the adoption of wireless technology in mobile commerce environment. This is mainly due to the sensitive and critical nature of user information and the lack of security offered by wireless IEEE802.11x based systems in the past.
While the size of mobile computing devices has been reduced in the recent years, the computing capacity that drives these devices has grown significantly. For instance, certain digital assistants come in smaller size and are capable of handling functions realised by word processors and spreadsheets. In addition, these devices can also handle a calendar, an address book and a small size memo pad. These were functions realised in a desktop computer a few years ago. Today's handheld devices have computing power almost equivalent to their desktop-computing counterparts of only one generation earlier. This phenomenon, while driving more and more functionality into handheld wireless Internet-enabled devices, is also driving security risks such as theft or loss of data specific to desktop computing into wireless devices, especially in the mobile computing applications arena. Some of the security risks highlighted in the literature include identity theft and credit card frauds (Kuechler & Grupe, 2003). Therefore, it is believed that failing to provide a secure system will significantly dampen consumer adoption rates of mobile commerce (Fink, 2000).

## TAXONOMY OF SECURITY ISSUES

Security appears to be assuming significant importance in the mobile commerce environment than a traditional electronic commerce environment because it is possible to eavesdrop into other's message with minimum difficulty in mobile environment (Gururajan & Vuori, 2003). In a connected medium, it is fairly difficult to penetrate networks that are secured. Further, due to the hardware capability of devices, it is possible to package more security applications on to these desktop devices. However, in a wireless environment, it is relatively easy to penetrate other devices because of the lack of security provided by certain wireless applications[1] due to hardware limitations. Therefore, the current architectures are trying to improve their design in terms of security. This has an impact for consumers because they are concerned about their data and voice messages from unauthorised access and expect security for data as well as for voice.
There are two major technical security concerns in a mobile commerce environment: *identification integrity*, and *message integrity*. The *identification integrity* refers to the signature elements found in the messages in order infer from where the message is originating. The *message integrity* refers to details in order to establish that the message is received as sent and no third party has attempted to

[1] Bluetooth provides a list of security issues in its discussion paper. Refer to www.bluetooth.com for more details.

open, modify or alter the contents. These two items appear to cause a lot of concern to both sender and receiver. The sender risks theft or misuse of their personnel information such as account and bank details and the receiver (usually a merchant) risks repudiation of the transaction and resultant non-payment. Data in mobile commerce environment is secured using encryption technology. It has been proven that the technology is vulnerable to attacks. Hackers have broken some of the existing algorithms for encryption. So, there is nothing like a complete security. The technical security threats can be categorised into threats that can impact data in a mobile commerce transaction environment, platform that facilitates this data communication and the software applications and protocols that are essential for such communication. These technical security risks can directly affect mobile commerce and these are discussed as 'direct security threats'. In addition to these direct threats, threats related to privacy issues, regulatory enforcement etc. can affect mobile commerce indirectly and these are discussed as 'indirect security threats'. These two broad classifications are explored below as shown in the following diagram.

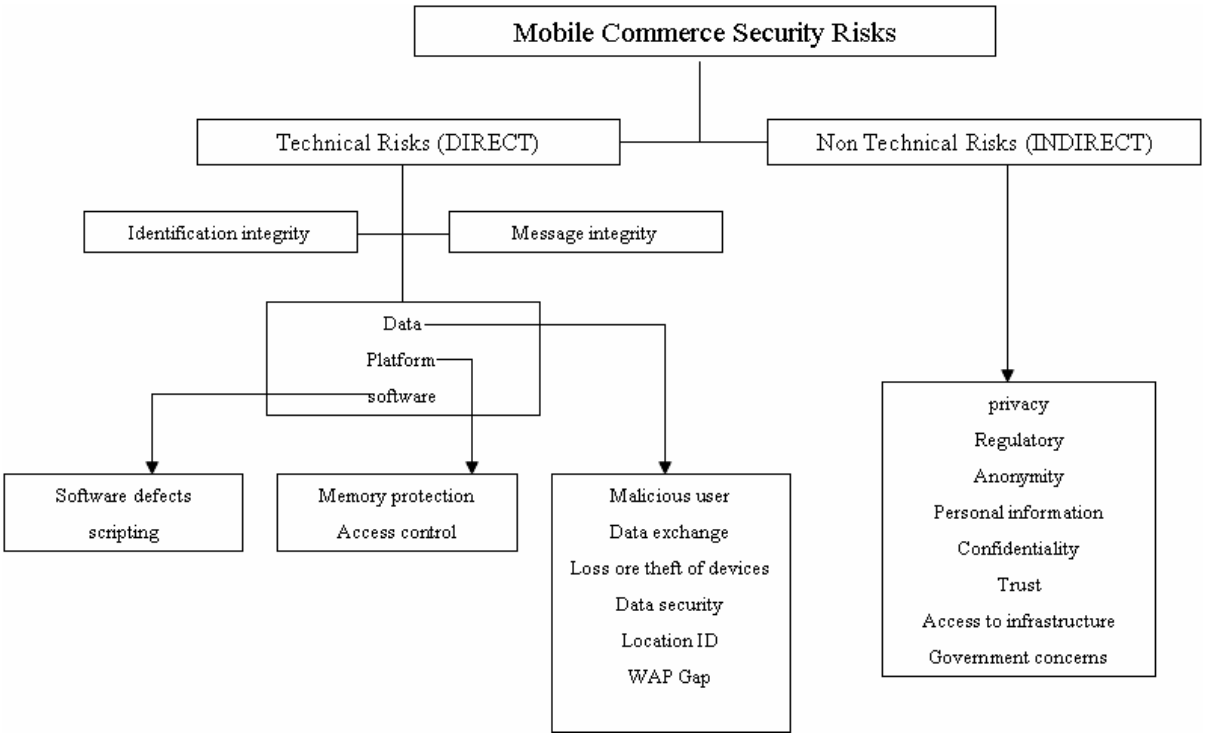


*Diagram 1: A snap shot of mobile commerce security risks*

## DIRECT SECURITY THREATS

Direct security threats are those that impact the users directly due to a technical issue, a data issue or a software application issue. Users may find it inconvenient to perform a mobile commerce transaction due to this direct risk. The data security risks specific to wireless computing would typically encompass malicious users, security problems with data exchange, loss or theft of devices, data security at transmission time, threat due to location identification and WAP Gap. The platform security risks involve memory protection and access control. The software risks involve software defects and scripting issues. These are elaborated in the following paragraphs.

### Data Security Risks

Malicious user

In addition to the usual Internet security threats of online applications, wireless computing introduces new hazards specific to mobility and communication medium. The very nature of the wireless computing facilitates the formation of ad hoc networks for the purpose of communication (Dornan, 2001). Ad hoc networks are formed for a specific communication and once the purpose is over, abolished. These ad hoc networks decentralise the decision-making processes because many such ad

hoc networks can be formed to take decisions. Users participating in these ad hoc networks connect their wireless devices such as notebook computers equipped with wireless protocols for the purpose of data transfer & exchange and these users are referred to as 'nodes' in the ad hoc network (Zhang & Lee, 2000). This decentralisation has resulted in network protocols that rely on cooperation among all participating devices. In these circumstances, an adversary node can exploit this assumed trust to compromise security. When such a security breach occurs, an adversary that compromises a single node can disseminate false routing information. This may have a detrimental effect on the complete network and users connected to the network. In the worst case, this adversary can instruct all routing to go through the compromised node (Zhang & Lee, 2000). Similarly, while mobile users roam through many different cells and ad hoc networks, the communication is handed off from one domain to the next. At this point, a single malicious domain can potentially compromise wireless devices by facilitating malicious download of data or programs. In certain cases, this may result in denial of service.

The mobile computing medium provides excellent cover for malicious users because wireless devices roam in and out of wireless zones, have no fixed geographic point, and can go online and offline easily (Atwal, 2001). This enables the users to very quickly disconnect from the network and when this happens it is difficult to establish the physical location of the user. Therefore, this 'roaming' makes it difficult to trace a mobile user. As a result, users with mobile devices can launch attacks against fixed networks easily where tracing an attack becomes difficult. Further, rather than an attacker needing to pursue a target, targets can come to attackers in wireless networks simply by roaming through the attacker's zone.

Wireless connections can be easily compromised even without exploiting ad hoc networks at the transport layer level (Young, 2000). This layer of the network can be loosely seen as the vehicle that transports user identities. For example, airline passengers who check their emails in airports during wait times using their mobile devices reveal their identity to the wireless networks. A malicious attacker can easily identify the passenger's details and can divert the passenger's web request to the malicious hacker's site. Since secure DNS has not been widely deployed in wireless computing, it would not be difficult to implement such a stealthy attack, providing the same look and feel of the Web site is as easy as downloading the target site Web pages. The insidious part of the attack involves discreetly changing dynamic information to the benefit of the malicious user or the detriment of the passenger.

Data exchange

While engaged in communication, wireless devices pass through many different, potentially non-trustworthy networks to derive various services (Turisco, 2000). While these services are realised, data are exchanged between the mobile user and the network. It is at this point that information can be stolen or altered without the mobile user's knowledge because of the visibility of the mobile user to the network. Further, transactions can be interrupted and then reinstated, often without proper authentication procedures which are usually strictly followed in a wired network (Schiller, 2000). This is because most vendor implementations of the Secure Sockets Layer (SSL) or its wireless counterpart, Wireless Transport Security Layer (WTSL) do not follow rigorous authentication procedures or perform standard checks once a connection has been established. Therefore, it is possible for a malicious attacker to redirect transaction requests without the user's knowledge thereby gaining access to user's information. Further, most web sites are not currently configured to deal with intermittent service failures, which is common with wireless connections and malicious attackers can use this vulnerability to their advantage in wireless networks.

Loss or theft

Another risk unique to mobile devices is the risk of loss or theft of devices due to their small size (Loney, 2000). Without physical security provided in a traditional network environment, mobile computing devices are at increased risk of theft and loss, particularly given their small size. While the data stored on a misplaced device might be irreplaceable, other risks of lost Internet-enabled devices include the ability for finders of lost devices to access proprietary corporate systems, including email servers and file systems. One of the key problems with the current generation of handheld devices is the lack of good mechanisms to authenticate a particular user to a particular device.

Data security

In addition to the issue of security, m-commerce applications introduce new and significant risks to data security. Users currently own their wireless devices such as cellular phones and PDAs. As a result, users enter their personal data on these devices as they would on corporate machines. When a user establishes a connection using the protocols supporting mobile communications, the user's data are revealed (Langley, 2000). In the current climate, major marketing and data collection firms track users' online Web usage by means of software programs similar to cookies. For example, in March 2000, it was disclosed that AT&T Wireless and Sprint PCS were sending users' phone numbers to the Web sites they accessed from their Web-enabled wireless phones (Sausser, 2003). As a result, these Web sites can now track end users by personal identity information such as phone numbers as well as potentially using those phone numbers for offline direct telemarketing.

Location id

Other data risks involve using location identification devices (Haskin, 1999). Location-oriented services provide the ability to determine a user's geographic location with a certain degree of precision, say within a range of 15 meters from the location of the mobile device. Therefore, it is possible to establish a user's geographic location. This identification of location may cause potential security risks. For instance, it is possible to steal data from a mobile device such as a mobile computer with wireless access based on this identification. In the past, the media has reported that stock exchange details were stolen from executives who access this data in airport terminals by this method.

WAP Gap Risk

The proponents of wireless applications argue that the Wireless Transport Security Layer (WTLS) provides a secure infrastructure for applications development (Clarke, 2003). When wireless requests are made to web pages of a network server, these requests are translated at the Wireless Application Protocol (WAP) gateway from the Wireless Transport Security Layer (WTSL) protocol to the standard Session Security Layer (SSL) protocol widely used in the secure Hyper Text Transfer Protocol (HTTP) requests. This process is commonly known as the "WAP Gap". In the process of translating one protocol to another, the data is decrypted and then re-encrypted. If an attacker is able to have access to the mobile network at this point, then simply capturing the data when it is decrypted can compromise the security of the session.

Malicious attackers tend to avoid the security provided by encryption protocols because of the strength of the perceived security elements of data encryption over communication channels. Therefore, these hackers tend to simply attack the weakest links in the system, such as servers and clients. There are currently few wireless gateways or portals to the wired Web. Thus, those few gateways present ideal targets of opportunity or single points of failure for an attacker to bring down a significant portion of the wireless Web by selective denial-of-service attacks.

**Platform security threats**

The basic infrastructure for running wireless applications is provided by the hardware platform. Therefore, without an infrastructure that fully supports security for computing applications on the device, achieving secure applications may not be possible (Schiller, 2000). In reality, the majority of the manufacturers of wireless devices has ignored this and has failed to include basic operating system security features. This has, in turn, lead to insecure applications. In general the failure to provide security features includes memory protection for processes, protected kernel rings, file access control, authentication of principals to resources, differentiated user and process privileges and biometrics authentication.

Memory protection

It is reported by Ghosh (2001) that one of the most popular PDA devices on the market does not provide memory protection for its applications and this has lead to serious threats for each application's own security and privacy. For instance, when a private key is used for a trusted application for the purpose of signing documents, attacks can be launched by a rogue application. The rogue application can attempt to steal the decrypted key in the signing application's memory by interrupting it at just the right moment. To resolve these platform risks, appropriate memory protection needs to be enforced between applications to prevent one application from being able to see another.

Access control

The second fundamental protection necessary is access control for objects to prevent unauthorised programs and users from accessing confidential data such as private keys or confidential information in databases (Stowe, 2000). Wireless PDA platforms should also support encrypted tunnels or virtual private networks to provide confidential access over insecure wireless links to corporate systems. Finally, strong authentication mechanisms such as fingerprint recognition systems should be built into the devices to authenticate the user to the device.

**Software security threats**

While the operating system provides the basic platform for wireless applications, the software applications that run on these devices are equally important. Assuming that basic platform services such as memory protection are provided to applications, it is possible to design and develop secure wireless applications using good software engineering and assurance methods. While the relation between software flaws and security vulnerabilities is well understood, it may still be possible to develop software applications with defects.

Software defects

The software defects or flaws in a mobile environment can occur in a number of ways (Stuart & Bawany, 2001). Firstly, flaws in the logic of a program and in the implementation of the program can result in security holes that will be exploited by attackers or malicious Web sites. Secondly, low-level languages used for the development of applications for handheld devices may still contain common flaws such as buffer overflow flaws. Thirdly, the physical limitations of a wireless device may impose certain security and performance trade-offs. For instance, limited power, processing cycles, memory, and bandwidth will force application developers to forgo security features, such as encryption, in an effort to improve online performance. Fourthly, vendors may ignore security features available in advanced languages such as Java due to developmental time constraints. For instance, runtime checking of type safety is expensive both in programming time and testing time and developers of software applications for wireless devices may ignore this aspect. Similarly, implementing fine-grained sandboxes and stack-introspection, some of the standard security features implemented in current desktop domain, may be ignored due to time and cost constraints.

Scripting

In addition to the above potential software development defects, scripting can introduce other run-time problems (Gururajan, 2001). One of the most interesting software-related developments in wireless devices is the ability to send and execute mobile code. In the traditional desktop environment, using Java applets, it is possible to move ‘code’ between machines. Further, scripting is used extensively in Web pages to validate forms and create the look and feel of Web pages. For several reasons, scripting will also have ample uses in the wireless Web. Client-side processing is attractive for reducing the number of communication hits necessary on extremely bandwidth-limited wireless links. For instance, client-side form validation reduces unnecessary server-side error reports and re-entry messages. Further, some server-side processing can be off-loaded to clients using mobile code that will increase the availability of servers to more simultaneous connections. In addition, scripting will be pervasive in wireless web computing for the same reason that it has become ubiquitous in wired Web pages: Web page development heavily leverages JavaScript for display functions and client-side transaction processing.

In summary, mobile e-commerce systems will introduce (directly) new security risks beyond those currently found in desktop e-commerce systems. Using wireless devices for m-commerce will result in new vulnerabilities and potentially represents a new weak link in the development of m-commerce. Since attackers tend to exploit the weakest link in a chain, the security risks of wireless devices must be carefully analysed and addressed.

**INDIRECT THREATS**

In addition to the three broad categories discussed above, namely, data threats, platform threats and software threats, it is possible to identify a number of indirect threats in a mobile commerce environment. For example, in a mobile communication environment the issue of privacy is discussed in great length due to the impact privacy has on users. Similarly, details on regulatory implications

associated with mobile commerce can also be found in the literature. These indirect threats have assumed importance in the recent months as they influence the adoption of the concept among users. These are discussed below.

**Privacy issues**

There is a general concern regarding the privacy of information available in an electronic commerce as well as mobile commerce environment (Shortliffe & Barnett, 2001). For example, in August 2001, it was reported in the West Australian media that local councils parted with ratepayer information to certain building contractors. While some council provided part information, other councils provided entire details such as house addresses, type of renovation undertaken etc. Therefore, the question of how much information is private arises. If ratepayers refuse to provide certain personal information, then local councils might restrict certain services. On the other hand, if certain personal details are given, authorities might disclose the information to other parties. It appears that health data have been sold to pharmaceutical manufacturers in various countries for a sizeable amount without the consent of patients. So, the issue of privacy assumes significance in mobile and electronic commerce environments.

In mobile commerce environment, due to the nature of transmission, it is possible to capture various details about consumers and then store it for analysis purposes (Yampel & Eskenazi, 2001). In recent reports, it has been highlighted the ease with which data can be stored during transmission in a wireless community. While the data is captured, the consumer may provide details of their personal life even without realizing the potential cause at a future point. Recent privacy issues involve children naively revealing their addresses or disclosing their parent's credit card details or other sensitive information to unauthorized personnel. This has also given raise to security issues. Many vendors have raised this concern.

In January 2000, it was reported in the Australian media that children who have access to mobile telephones used the services offered beyond their paying capabilities. These children were sent accounts, which they were unable to pay, so the telephone companies considered their parents and/or guardians to be legally responsible for the debts and asked them to pay. This has opened another interesting issue in terms of privacy. How much information is private? Can we restrict or prohibit certain services based on certain criteria? In this case, if we restrict the usage of mobile telephones, then in emergency situations, these children would have no access to help. On the other hand, if we fail to restrict the use of these devices, the services are over used and payment difficulties result.

The wireless technologies' surveillance capacity to collect, aggregate, analyse and distribute personal information coupled with current business practices have left individual privacy unprotected. While recent surveys and public pressure have raised the privacy consciousness of companies, particularly those operating online, individuals' information is frequently used and disclosed for purposes well beyond what the individual provided it for.

It appears that in Australia privacy concerns are not fully resolved. In Australia, all government agency web sites should contain a privacy statement or disclose their privacy policy. It appears that this issue has not yet been fully resolved. The privacy policy should detail what information a web site is going to collect, how it would be used and whether it would be disclosed to third parties, including other government agencies. While this requirement gives a feeling that the consumers are guarded, making changes to existing policies on a web page or encouraging consumers to read those policies in practically not possible. This will also not constitute 'adequate notification' as warranted in privacy legislation.

In 1999, the Internet Industry Association of Australia produced an Internet Industry Code of Practice. One of the aims of that Code is to "establish confidence in and encourage the use of the Internet". As part of that aim, the Code includes a requirement for all parties subscribing to the Code to provide details on their website of their Australian Company Number, their physical office address and contact telephone number, when entering into a transaction with a user. It also includes a prohibition on engaging in conduct which is misleading or deceptive, unconscionable or exploitative.

It is noteworthy to look at the weak state of privacy protections applied on documents. The national laws protect private papers. However, with the advent of home computers, individual diaries are moved to the desktop and to the hard drive. Further, network computing allows individuals to rent space outside their home to store personal files and personal World Wide Web pages. Storing personal information on a remote server eliminates many of the privacy protections afforded in a

physical world. In many countries, an individual's thoughts recorded electronically on a remote computer may be obtained from the service provider through a mere court order with no notice to the individual at all.

The weak state of privacy protection is evident in the business setting too (Lee, 2000). In the health industry, physicians are using intranets to enable the sharing of patient, clinical, financial, and administrative data. Built on Internet technologies and protocols, the private networks link the hospital's information system to other associated systems such as the pharmacy systems. In Australia, the government has access to the computer-based patient record system throughout the nation for financial assistance. Further, private sector companies are moving to integrate this data with commercial ideas.

Using wireless technologies, it is possible to move these records out of our doctor's offices using ad-hoc networks formed for the purpose of consultation. While the use of network technology promises to bring information to the fingertips of medical providers when they need it most, privacy concerns are also raised because the identification schemes of persons who access these information sources is not fool-proof.

In the absence of comprehensive national legislation to protect patient privacy, the legal protections afforded to individual's data may vary greatly depending upon how the network is structured, where data is stored, and how long it is kept. If records are housed on the computer of an individual service provider such as a doctor, then access to that data will be governed by national legislation. Law enforcement would be required to serve the individual service provider with a warrant and this service provider would receive notice and have the chance to halt an inappropriate search. Under national law, the consumer however, would receive no notice and have no opportunity to contest the production of the records. When information is in transit between a service provider and an organisation through a network, law enforcement's access is governed by the warrant requirements of the national electronic communications act. In this case, neither the service provider nor the consumer receives prior or contemporaneous notice. If the records are stored on a server leased from an Internet service provider, the protections are unclear. They may be accessible by mere subpoena. If they are covered by the "remote computing" provisions of national telecommunications act, this would severely undermine privacy in the digital age.

**Regulatory Framework**

There is no international regulatory framework available to enforce certain security-related problems. For example, when there is a security breach, there are no clear guidelines as to the guarantee of security to consumers. Further, when the security breach appears in an international transaction, the guidelines do not stipulate as to which country is responsible to prosecute the vandals.

Reports (Green, 2000) indicate that consumers are worried about their privacy and the potential intrusion when mobile devices are used. With certain financial transactions, consumers like to be anonymous, but this anonymity can be revealed in a mobile commerce environment because of location identification devices. In areas such as health, revealing patient details may violate privacy regulations in certain countries. While some governments are in the process of modifying their privacy laws, more work is needed to tighten the various loopholes caused by modern technologies. The following three issues – expectation of anonymity, control over personal information and expectation of confidentiality – will detail how privacy of an individual can be affected in a mobile commerce environment and how recent changes to privacy regulations safeguard individual privacy and potential security threat.

Anonymity

There is a general expectation from individuals that their anonymity will be protected when they communicate over the Internet, irrespective of their method of connectivity (Koller, 2000). If an individual has not actively disclosed information about himself or herself, then the expectation is that no one knows about the individual's identity. However, due to the possibilities of generation of an elaborate trail of data in the wireless arena, it is not always possible for an individual to assume that the anonymity is guaranteed. The individual's profile can be captured via transactional data, click stream data, or 'mouse-droppings', and this reveals an individual's online life.

For example, in the connected medium, technologies such as "cookies," enable Web sites to surreptitiously collect information about one's online activities and store it for future use. In a mobile

commerce environment, these cookies can be replaced with locator devices such as “Cell-Loc”. These locator devices are capable of identifying the location of a wireless device such as mobile telephones and hence its user. It appears that these locator devices are so powerful and accurate that it is possible to identify a device with a precision of 15 metres from its location. Initially, designed for the benign purpose of enabling employers to recognize an end user for responses, these locator devices are posing threat to one’s anonymity and hence privacy. In a mobile commerce environment, these locator devices facilitate the tracking and monitoring of specific individual's activities. The surreptitious collection of information about individual's activities, across multiple locations enabled through some locator device implementations, gained the attention of marketing professionals to target end users for online advertising.

This has resulted in a battle being waged today, over the "location" information available through many cellular networks, foreshadowing the larger privacy considerations lurking in the vast data generated by individuals' use of wireless devices (Deise et al., 2000). In the course of processing calls, many wireless communications systems collect information about the cell site and location of the person making or receiving a call. Location information may be captured when the mobile device is merely on, even if it is not handling a call. Both government and the private sector have their eye on this location information. While the government seeks to build added surveillance features into the network and ensure their access to the increasingly detailed data it captures, the private sector is considering how to use this new form of information. For example, a company in Japan is experimenting with a World Wide Web site that allows anyone to locate a phone, and the person carrying it, by merely typing in the phone number. A newspaper aptly published this as ‘Cellular telephones, long associated with untethered freedom, are becoming silent leashes’. It was also reported on 7 May 2001 in ‘The Australian’ that privacy laws warrant that companies get consumers’ consent prior to sending text advertisement messages to mobile phones. This regulation is in operation in Australia now. This regulation has opened up two major implications. Firstly, companies who do not comply with this regulation will be asked to do so by the national privacy commissioner to change their policies. Secondly, in more serious cases, where divulging personal details resulted in the loss of a job or discrimination, consumers could claim restitution in the civil courts. Therefore, employers would have to safeguard, update and hand over personal information such as an individual’s resume and work history, including opinions about their ability, if requested by an employee. The aim of this regulation was for consumers to control their personal information and the use of this personal information by private companies. It also appears that consent would be the key to determine whether a breach has occurred or not.

Control over Personal Information

When individuals provide information during a transaction, for example to a doctor, they expect that the information collected will be used for the sole purpose of providing the service requested. Unfortunately, current practices, both offline and online, foil this expectation of privacy. Information generated in the course of a business transaction is routinely used for a variety of other purposes without the individual's knowledge or consent. There are instances where some entities go so far as to declare the information individuals provide them as company "property."

There are multiple examples of companies using and disclosing personal information for purposes well beyond what the individual intended. For example, recent news stories in the US have focused the public on misuses of personal health information by the private sector, particularly when it is digitised, stored and manipulated.

There are number of incidents where personal information of individuals is disclosed without any proper consent (Simpson, 2003). For example, in 1996, Yahoo faced a public outcry over its People Search service. The service, jointly run with a marketing list vendor, would have allowed Net searchers to put an instant finger on 175 million people, all culled from commercial mailing lists. Later, Yahoo decided to delete 85 million records containing unlisted home addresses.

During August of 1997, American Online ("AOL") announced plans to disclose its subscribers' telephone numbers to business partners for telemarketing. AOL heard loud objections from subscribers and advocates opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information. In response, AOL decided not to follow through with its proposal. At the beginning of the year, the Washington Post reported that several states had entered into agreements to sell state drivers' license photos to Image data. Under public

scrutiny the deal seemed quite different, state governors and legislatures quickly moved to block the contract. In Australia, there is concern over the planned sale of patient's health records collected through pharmaceutical institutions t o undisclosed commercial companies (reported in the Australian, 27 February 2001).

There are operational difficulties in the implementation of obtaining consent from consumers. While most web sites use the 'click' method to acquire consent, the privacy laws appear to be aiming at more than this 'click' method. Visitors to a web site might be confronted with an upfront explanation and then be required to click their consent at the end of each page of information display or at the end of each section, realising unnecessary delays every time information is provided. Further, for auditing purposes, these keystrokes need to be logged and saved. The National Electronic Authentication Council (NEAC) also has highlighted deficiencies in the current privacy laws relating to the relationship between parties involved in Public Key Infrastructure (PKI). This issue is not yet fully addressed and only recently banking industries have accepted to follow a uniform PKIU policy.

Confidentiality

When individuals send an e-mail message, the expectation is that it will be read only by the intended recipient (Dang, 2000). Unfortunately, this expectation is not fully met by the existing wireless technology. If an individual is using wireless devices provided by the organisation, then it is possible, and legal, for the employer to monitor these devices, leading to non-assurance of privacy. Further, in a wireless environment, it is possible for a third party to capture the email, read, alter the contents and then transmit to the original recipient.

While domestic law provides e-mail the same legal protection as a first class letter, the technology leaves unencrypted e-mail as vulnerable as a postcard (Lee, 2000). Compared to a letter, an e-mail message travels in a relatively unpredictable and unregulated environment. In a wireless environment, due to intermediaries taking an active part in transmitting data, wireless emails can hop through a number of networks. As it travels through these networks, wireless e-mail is handled by many independent entities, whereas a letter is handled only by the postal service. To further complicate matters, the e-mail message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the statutory privacy protections stop at the border because of domestic laws and their jurisdiction. In addition, the Internet does not have central points of control and while the decentralised nature of the Internet allows it to cope with problems and failures in any given computer network, by simply routing in another direction, it also provides ample opportunities for those seeking to capture confidential communications. Policy of a single computer network can compromise the confidentiality of information. Users in mobile commerce environment can avoid these risks by implementing filters and other authentication techniques to avoid unauthorised access to their emails.

**Trust**

Trust is central to any commercial transaction and more so in the case of electronic commerce. Trust is normally generated through relationships between transacting parties, familiarity with procedures, or redress mechanisms. In the case of electronic commerce, the need for creating trust in the consumer is all the more important because of its virtual nature. It hinges on assuring consumers and businesses that their use of network services is secure and reliable, that their transactions are safe, that they will be able to verify important information about transactions and the transacting parties such as origin, receipt, integrity of information, and identification. Therefore the challenge is not to make e-commerce fool-proof but to make the system reliable enough so that the value greatly exceeds the risk. According to Fink (2000), there are three major issues as to why trust is very important for e-commerce. They are (1) the diverse nature of e-commerce (Mayer et al., 1995), (2) the extensive use of supply chain (Powell, 1997) and (3) the move towards self-directed work teams and the empowerment of workers (Hope-Ross, 2001). OECD in its report[2] entitled 'Dismantling the Barriers of Global Electronic Commerce' has listed *building trust* as one of the key aspects that would require more attention.

Hitherto, governments have played a major role in helping to create trust in economic transactions. But, in this rapidly changing information technology era, the private sector plays an increasingly

[2] More information can be found at: OECD web site http://www.oecd/org/dsti/sti/it/ec/prod/dismantl.htm

important role. Industry is called upon to develop technological solutions to meet the needs of businesses and consumers for different levels of security, certification, privacy and consumer redress. Governments are attempting to implement technology-neutral policies in order not to limit mobile commerce (including electronic commerce) business transactions (http://www.oecd/org/dsti/sti/it/ec/prod/dismantl.htm). According to Fink (2000), creating Web trust is more important because the parties are not in physical proximity and cannot observe body language.

Any new development in technology in today's consumer minds creates both curiosity as well as reluctance. Fink (Fink, 1998) stated that the informality and lack of overall control creates the perception that the Internet is inherently insecure. Business risks, such as products and services, inadequate legal provisions, reliability of trading partners, behaviour of staff and the demise of Internet service providers, and technological risks such as hackers, computer viruses, data interception and misrepresentation are all increasing. To achieve a satisfactory level of trust, one has to manage both the business and the technological risks. Fink (2000, p.38) suggests that the collective trust requirement for e-commerce can be met by one or more of three forms of trust, namely *deterrence-*, *knowledge-*, and *identification-based trust*. He further states that currently e-commerce relies mostly on knowledge-based trust, as in the case of EDI systems that are useful for Business-to-Business commerce. However, there is now a surge in identification-based trust which is provided by security guaranteeing organisations such as WebTrust whose seal of trust indicates to the consumer that the particular Web site has a high level of security and integrity. Specifically, Web Trust addresses three broad areas of risk with electronic commerce, these are business practices, transaction integrity and information protection. But when trust is not fully guaranteed in the wired medium through which e-commerce currently operates, how is it possible to guarantee trust in a wireless medium? For instance, the current architecture for wireless communications does not provide full trust in terms of transaction integrity. Some of the models envisaged for m-commerce are based on a smart card approach and hence the issue of trust needs greater examination in m-commerce.

**Access to and Use of Infrastructure**

Despite the technical development, access to the infrastructure on which m-commerce is to be developed is essential. Some of the major issues related to access and use of infrastructure are: technical neutrality, skills, radio-frequency availability and the cost associated with services (Schiller, 2000).

The concept of technology neutrality refers to the availability of technology for the implementation of various services to facilitate e- and m-commerce. For instance, encryption techniques differ between countries and there are no government regulations to stipulate a neutral technology to facilitate international transactions. While there is a minimum standard available, the neutrality of such standards is questioned. Such differences will hinder development (Ross, 2000).

Skills in IT are a worldwide problem. When new technologies are introduced, users need to acquire skills to use these technologies. In addition to this, skills are needed to develop the technology. Despite the publicity about mobile computing since 1994, and the existence wireless applications since 1998, consumer products are not freely available. This is a concern (Ridge, 1999).

The question of operating frequency for wireless communication and hence m-commerce is a confusing issue. There are three groupings available in terms of use of radio frequency. For instance, the standard 2.4 M frequency is used free of cost in a number of countries. Countries such as France, which operate their military radio frequency at this level, do not allow use of this radio frequency. Consumers will be affected by this (Sausser, 2003).

Due to the infant stages of both e-commerce and m-commerce, the issue of cost has not been fully explored. Despite the availability of certain economic models for Internet pricing, the cost of infrastructure to facilitate such services has not been fully examined. Such an examination throws a number of questions open: Who is going to pay the cost – businesses or consumers or governments? How does the pricing mechanism evolve – based on volume or transaction? These questions are yet to be raised fully and answered and until such time that they are, the development and hence the implementation of the m-commerce domain is not fully complete.

**Government Concerns**

In the m-commerce environment, governments are concerned with regulatory frameworks. The United Nation's UNCITRAL Model Law serves the basis for a number of countries to modify their existing laws to accommodate e-commerce. When m-commerce is realised, these laws will need to undergo further revision to suit m-commerce applications, their implementations and consumers. Some of the concerns governments are currently facing are the international regulatory framework, encryption standards, technology neutrality, digital currency backup and the provision of intermediary services to support m-commerce development especially in the communications arena.

Jurisdictional Issues

Just as electronic commerce opens up new opportunities for international trade, it also opens up new questions regarding the application of laws to transactions conducted wholly or partially on-line. The ACCC has already noted an increase in complaints received from Australian consumers regarding products and services purchased from other countries as well as complaints from overseas consumers about products purchased from Australia. Consumer complaints regarding purchases made over the Internet from overseas entities are difficult to resolve on an individual basis because of questions about jurisdiction, enforceability and resultant costs and delays. Regulations such as the place of transaction and the law of contract are made obsolete by the borderless nature of the Internet. Unscrupulous traders will find it easy to avoid regulation in the electronic marketplace without a cooperative global approach to these issues (Freeman, 2003).

Taxation

In Australia, the viability of electronic commerce will be at least partially determined by the tax regime. The US has taken the position that there should be "no discriminatory taxation against Internet commerce". In particular, it advocates that the Internet should be a tariff-free zone. But the Australian Tax Office (ATO) Report[3] of 1999 notes that the tariff-free policy advocated by the US does not extend to tangible products ordered and paid for on-line but delivered in the conventional manner.

The ATO Report follows an extensive review of the impact of electronic commerce on the Australian taxation system. The Report is intended to stimulate further discussion at both national and international levels, prior to formulating the ATO's final recommendations to the Australian government. The Report states that the key principles of international taxation, such as source of income, residency and place of permanent establishment are "seriously challenged" by the emergence of electronic commerce.

Some of the key findings mentioned in the report include:

- The lack of legal infrastructure
- A reliable and easy electronic payment system
- The varying impact of the taxation system of e-commerce
- The application of jurisdiction, and
- Encryption difficulties in terms of Crime and Tax Evasion.

The Report makes a number of recommendations on the basis of these findings. Of particular relevance is the need for international consultation and cooperation with respect to the regulation of electronic commerce and the enforcement of taxation laws. The Report also recognises that taxation policies associated with electronic commerce should be developed in cooperation with other federal government agencies who are currently examining a range of other issues related to the on-line environment.

The Report recognises that "the ATO should be sensitive to the effect of e-commerce regulation on the nascent Internet commerce industry in Australia". It also makes a number of recommendations for the industry that may be regarded as controversial. For example, the ATO advocates the licensing of both `web shops' and organisations that operate or host web shops. In order to ensure a greater degree of control over tax reporting a framework to monitor commercial Internet traffic should be established. As part of this process, a record of the range of IP addresses assigned to Australian based computers should be maintained and the reporting requirements relating to a 'cash dealer' under the Financial Transactions Reports Act 1988 should be reviewed to capture digital cash transactions. The ATO should also negotiate with software manufacturers regarding the inclusion of some form of 'date

[3] The report can be found in ATO's web site www.ato.gov.au

stamping' or other means of ensuring the integrity of transactional records in software used for electronic commerce. The Report also recommends that major international credit card and other electronic payment system providers should be requested to provide access to transaction records held outside Australia. The efficient functioning of electronic commerce requires all of these issues to be dealt with in ways that are both technology neutral and which have worldwide endorsement and recognition.

International harmony is another aspect that needs consideration. Due to implementation issues, national laws may differ from international regulations in certain cases. For instance, custom regulations in certain countries demand print medium while in certain other countries electronic documents are allowed. In addition to this, the implementation of regulations differs from country to country, for example, in the area of encryption,. This variation can cause potential problems in technology use and access. Thus, international harmony is important in e-commerce and in developing m-commerce.

## CONCLUSION

While many of the risks of desktop computing will be found in wireless computing, the nature of the wireless medium requires a degree of trust and cooperation between member nodes in networks. If this cooperation is not guaranteed, then a malicious user can exploit the weakness in order to either deny service or collect confidential information or disseminate false information. Furthermore, the platforms and languages being developed for wireless devices appear to have failed to adopt the fundamental security concepts employed in the current generation of desktop machines. Probably the most significant risk could be from malicious code that is beginning to penetrate wireless networks, and which has the ability to undermine other security technologies such as signing, authentication, and encryption because it runs resident to the device with all the privileges of the owner. The security threats presented by malicious mobile scripts to wireless computing also appear to be significant. Therefore, device manufacturers and language developers for wireless applications should attempt to produce secure operating system models and secure models of computation before going forward with business-critical and privacy-related wireless applications.

Apart from the direct threats, in the current climate, the indirect threats are also assuming importance due to issues such as amendments to privacy regulations. Therefore, attention needs to be paid in order to monitor and control the indirect issues discussed in this paper. Otherwise, we are expected to repeat the mistakes of the past, and potentially take two steps backward as we move one step forward.

## REFERENCES


Atwal, R. (2001). *The wireless office: Evolution, Revolution or Bust* (No. PCIS-EU-DP-0101): Gartner Research.

Clarke, R. (2003). *Identification and Authentication Fundamentals*. Retrieved 10 Feb 2004, 2004

Colagiuiri. (1997). Integrating patient records and health information management systems. *Asia Pacific Hospital, 202*, 14-15.

Dang, A. V. (2000). *Four action items for E-Business: Transaction Security* (Research Note): Gartner Advisory.

Deise, M. V., Nowikow, C., King, P., & Wright, A. (2000). *Executive's Guide to e-Business: From Tactics to Strategy*. New York: John Wiley & Sons, Inc.

Deitel, D., & Deitel, N. (2001). *e-Business and e-Commerce - How to program*. New Jersey: Prentice Hall.

Dornan, R. (2001). *The essential guide to wireless communication applications*. Upper Saddle River, NJ: Prentice Hall PTR.

Fink, D. (1998). *E-Commerce Security*. Sydney: CCH Publishers.

Fink, D. (2000). Developing trust for Electronic Commerce. In L. Janczewski (Ed.), *Internet and Intranet: Security and Management: Risks and Solutions* (pp. 44-86): Idea Group Publishing.

Freeman, E. H. (2003). Privacy Notices under the Gramm-Leach-Bliley Act. *Legally Speaking*(May/June), 5-9.

Ghosh, A. K. (2001). *Security and Privacy for E-Business*. New York: Wiley.

Green, P. (2000, 4 June). Eastern Europe's Foray into M-Commerce. *The New York Times*, p. 3.8.
Gururajan, R. (2001). *Wireless Applications: Influences and Risks of Location Identification Technologies.* Paper presented at the Australian Conference on Information Systems, Coffs Harbour, NSW.
Gururajan, R., & Vuori, T. (2003). *Experiences in Wireless Application Development in a Healthcare Setting.* Paper presented at the WeB 2003, Perth, Australia.
Haskin, D. (1999). *Analysts: Smartphones to lead e-commerce explosion* (No. 991103ecomm): Gartner Research.
Hope-Ross, D. (2001). *Successful E-Business Deployment: Beyond Software* (No. COM-14-5080): Gartner.
Hu, P. J., Chau, P. Y. K., & Liu Sheng, O. R. (2002). Adoption of telemedicine technology by health care organisations: An exploratory study. *Journal of organisational computing and electronic commerce, 12*(3), 197-222.
Koller, L. (2000). Banks flirting with wireless billing. *Bank Technology News, 13,* 25.
Kuechler, W., & Grupe, F. H. (2003). Digital Signatures: A Business View. *Information Systems Management*(Winter 2003), 19-28.
Langley, N. (2000, May 11). Get moving on m-commerce. *Computer Weekly,* 68.
Lee, A. (2000). Small firms must take Internet plunge or risk being sidelined. *The Engineer, 10*(November 2000), 10.
Loney, M. (2000). M-Commerce safety fears. *IT Week, 3,* 6.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organisation trust. *Academy of Management Review, 20*(3), 709-734.
McConnel, B. (2000). Kennard pushes cable DTV. *Broadcasting & Cable*(February), 37.
Powell, M. (1997). Electronic Commerce: An overview of teh legal and regulatory issues. *International Trade Law and Regulation, 3*(3), 85-93.
Redman, P. (2002). *Wait to Invest in Next-Generation Wireless Services* (Research Note No. T-15-2354): Gartner Research.
Ridge, J. (1999, 9 November). Benefits for all in traineeship. *The Australian*.
Ross, B. (2000). CBS. *Broadcasting & Cable*(February), 38.
Sausser, G. D. (2003). Thin is in: web-based systems enhance security, clinical quality. *Healthcare Financial Management, 57*(7), 86-88.
Schiller, J. (2000). *Mobile Communications*. New York: Addison-Wesley.
Shortliffe, E. H., & Barnett, G. O. (Eds.). (2001). *Medical data: their acquisition, storage and use* (Second ed.).
Simpson, R. L. (2003). The patient's point of view -- IT matters. *Nursing Administration Quarterly, 27*(3), 254-256.
Stowe, B. (2000). Wireless networking looks attractive, but what about the cost of keeping it secure? *Infoworld*(May), 92.
Stuart, D., & Bawany, K. (2001). *Wireless Services: United Kingdom* (Operational Management Report No. DPRO-90741): Gartner.
Turisco, F. (2000). Mobile computing is next technology frontier for health providers. *Healthcare Financial Management, 54*(11), 78 - 82.
Yampel, T., & Eskenazi, S. (2001). New GUI tools reduce time to migrate healthcare applications to wireless. *Healthcare Review, 14*(3), 15-16.
Young, D. (2000). Handicapping M-Commerce: Getting ready for wireless e-commerce. *Wireless Review*(August), 24-30.
Zhang, Y., & Lee, W. (2000). *Intrusion detection in wireless ad-hoc networks.* Paper presented at the ACM/IEEE MobiCom.

[i] The term ‘risk’ is interchangeably used with ‘threat’ in this paper